Use ProjectPlace APIs

ProjectPlace exposes some of its data through an Application Programming Interface (API). It allows third-party developers to develop integrations, addons and applications based on the ProjectPlace service.

RESTful APIs

Anything that can be done in the ProjectPlace application can also be done programmatically via APIs by any developer. Please refer to the API documentation for more information about our RESTful API endpoints.

In order to get started using the ProjectPlace APIs; refer to our page on Developer Settings.

Organisational accounts can set up special integration accounts - also known as "robots" for use in business-to-business integrations. Robots are super users which cannot be used to sign in to the service - but can only be used to access and modify resources programmatically (via the APIs). See our page on how to Manage robots in your account for more information.

OData-endpoints

ProjectPlace exposes plenty of information via OData endpoints. These endpoints are typically intended for use with reporting software such as PowerBI or Tableau. The OData endpoints can be accessed via OAuth1, OAuth2 or Basic Auth for OData. OAuth1 and OAuth2 are covered in our API documentation site.

- See here for information on our OData endpoints
- See here for information about our OData solutions specifically targeted toward PowerBI

Basic Auth for OData

Some tools on the market do not support OAuth1 or OAuth2 access to OData endpoints out of the box. One popular example is the Tableau. These tools typically only support what is known as Basic Authentication - which is basically only username and password sent directly to the tool. This is a significant security risk for many reasons the main being that third parties would have to store user passwords in order to function. Third parties may be breached, and if malicious may use credentials for undisclosed purposes.

The good news is that you can still use basic authentication for tools such as Tableau. However, a special purpose app password must first be generated. These app passwords only grant access to OData (which minimizes the attack surface) and they also expire every 90 days, minimising the time during which a compromised app password can be used.

To use app passwords for OData access, the feature must first be made accessible to specific users in your account. Send a support ticket to us detailing who should have access to generate app passwords for OData access. You can only

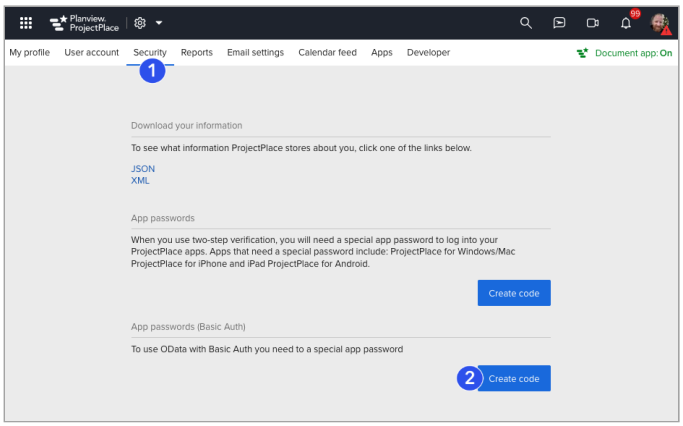
specify people who are actually a part of your ProjectPlace organisation.

Once the feature has been activated instruct them to:

1. Go to **User Settings** > **Security**
2. Click **Create code**
3. The **app password** will be displayed on screen - it will be displayed only once.
4. The app password can be **deleted at any time** by the user.

The app password is valid for 90 days - after which a new app password will have to be generated. Once an app password has been obtained - it can be used together with the user's email-address to access our OData endpoints via for example Tableau or Excel.

Never send your actual password to third party services. Other authentication standards (e.g OAuth and Single Sign On via SAML) exist in order to prevent the dissemination of actual user credentials.



- Was this article helpful?

- Yes
- No
- Leave feedback
-

Leave feedback
How can we improve this article? Please include your e-mail address if you would like us to contact you.

Submit feedback